UNITED STATES DISTRICT COURT

for the

Northern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

5003 Garden Drive
Hutchins, Texas

Case No. 4:16-mj-761

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment "A"

located in the Northern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252 and 2252A	Possession, Receipt, and/or Distribution of Child Pornography

The application is based on these facts:

See Attached Affivadit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Kyle L. Kuykendall, Special Agent, ICE
Printed name and title

Sworn to before me and signed in my presence.

Date: 12/12/16

Judge's signature

City and state: Fort Worth, Texas

United States Magistrate Judge Jeffrey L. Cureton
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Kyle L. Kuykendall, a Special Agent of the United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), being duly sworn under oath, do hereby depose and state:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), assigned to the Special Agent in Charge, Dallas, Texas. I have been employed with HSI since August of 2008. As part of my duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have been involved in numerous child pornography investigations and am very familiar with the tactics used by child pornography offenders who collect and distribute child pornographic material.

2. As a federal agent, I am authorized to investigate violations of the law of the United States and to execute warrants issued under the authority of the United States.

3. This affidavit is being made in support of an application for a search warrant for the residence located at **5003 Garden Drive, Hutchins, Texas**, for the items specified in Attachment B hereto.

4. The statements in this Affidavit are based in part on my investigation of this matter and on information provided by other law enforcement agents. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252, and 2252A, is located within the account identified in Attachment A.

5. The purpose of this application is to seize evidence, more particularly described in Attachment B, of violations of 18 U.S.C. §§ 2252 and 2252A, which make it a crime to possess, receive, or distribute child pornography.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

7. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

8. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

9. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

10. "Internet Service Providers" or "ISPs" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

11. "Electronic Mail," commonly referred to as e-mail (or e-mail), is a method of exchanging digital messages from an author to one or more recipients. Modern e-mail operates across the Internet or other computer networks. E-mail systems are based on a store-and-forward model: e-mail servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need only connect briefly, typically to an e-mail server, for as long as it takes to send or receive messages. An Internet e-mail message generally consists of three components, the message envelope, the message header, and the message body, but may include a fourth component, an attachment. E-mail attachments can include any type of digital file. There are numerous methods of obtaining an e-mail account; some of these include e-mail accounts issued by an employer or school. One of the most commons methods of obtaining an e-mail account is through a free web-based e-mail provider such as, MSN, Yahoo, or Gmail. Anyone that has access to the Internet can generally obtained a free web-based e-mail account.

12. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video

disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND REGARDING THE USE OF INTERNET/COMPUTERS/CELLULAR PHONES AND CHILD PORNOGRAPHY

13. I have been formally trained in the investigation of crimes involving the online sexual exploitation of children and have been investigating these crimes since 2009. Based on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know the following:

14. The Internet is a worldwide computer network that connects computers and cellular phones and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider ("ISP") that connects to the Internet. The ISP assigns each user an Internet Protocol ("IP") Address. Each IP address is unique. Every computer or device, to include a cellular phone, on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer or cellular phone from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers.

Most ISP's employ dynamic IP addressing; that is, they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.

15. With advent of digital cameras, including those found on "smart" cellular phones, child pornographers can now transfer photographs from a camera or a "smart" cellular phone directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers and cellular phones around the world. The ability to produce child pornography easily, reproduce it inexpensively, and distribute it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer or cellular phone and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

16. The computer or cellular phone's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy or compact disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 250 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

17. With Internet access, a computer or "smart" cellular phone user can transport an image file from the Internet or from another user's computer or cellular phone to his own device, so that the image file is stored in his device. The process of transporting an image file to one's own computer is called "downloading." The user can then display the image file on his computer screen, and can choose to "save" the image on his computer and/or print out a hard copy of the image by using a printer device (such as a laser or inkjet printer).

18. Importantly, digital files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.

Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

USE OF FINGERPRINT ENABLED SECURITY ON MODERN DIGITAL DEVICES

19. As discussed herein, based on my training and experience I believe that digital devices will be found during the search. I know from my training and experience and my review of publicly available materials that Apple Inc., Motorola, HTC, and Samsung, among other companies, produce devices that can be unlocked by the user with a

numerical or an alpha-numerical password, or, for some newer versions of the devices, with a fingerprint placed on a fingerprint sensor. Each company has a different name for its fingerprint sensor feature; for example, Apple's is called "Touch ID." Once a user has set up the fingerprint sensor feature in the security settings of the device, the user can unlock the device by placing a finger or thumb on the device's fingerprint sensor. If that sensor recognizes the fingerprint or thumbprint, the device unlocks.

20. Most devices can be set up to recognize multiple prints, so that different prints, not necessarily from the same person, will unlock the device. In my training and experience, users of devices with a fingerprint sensor feature often enable that feature, because it unlocks the phone more quickly than the entry of a passcode or password but still offers a layer of security.

21. In some circumstances, fingerprint sensors will not work, and a passcode must be entered to unlock the device. For example, with Apple, Touch ID will not work if (1) more than 48 hours have passed since the device has been unlocked, (2) the device has been turned on or restarted, (3) the device has received a remote lock command, or (4) five attempts to match a fingerprint have been unsuccessful. Other brands have a similar restrictions. I do not know the passcodes of the devices likely to be found at the Subject Premises.

22. For these reasons, while executing the warrant, agents will likely need to use the fingerprints or thumbprints of any user(s) of any fingerprint sensor-enabled device(s) to attempt to gain access to that device while executing the search warrant.

23. The warrant seeks the authority to compel the use of the fingerprint and/or thumbprint of every person who is located at the Subject Premises during the execution of the search and who is reasonably believed by law enforcement to be a user of a fingerprint sensor-enabled device that is located at the Subject Premises and falls within the scope of the warrant. The government may not be able to obtain the contents of the devices if those fingerprints are not used to access the devices by depressing them against the fingerprint sensor at the time of the search.

24. Although I do not know which of the fingers are authorized to access on any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors, and in any event all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

BACKGROUND OF INVESTIGATION

25. On November 20, 2015, in Indian Head Saskatchewan, Canada, a 14-year-old minor female victim contacted an investigator with the Royal Canadian Mounted Police (RCMP) to inform them that she had been the victim of extortion. She alleged that while utilizing the social media application "KIK Messenger" on her cellular phone, she entered into a conversation with an unknown person utilizing the username "**itsmeyall1**."

26. The user of "**itsmeyall1**" identified himself/herself as a fourteen-year-old female and encouraged the minor female victim to exchange photographs. The initial request was for images of the minor female victim's face, but subsequent requests progressed to explicit images of the minor female both in her underwear and with her genitals exposed.

The user of "**itsmeyall1**" would respond by sending the minor female victim photographs of a similarly aged female engaging in similar behavior. During the conversations between the minor female victim and the user of "**itsmeyall1**," the user of "**itsmeyall1**" provided his/her phone number as **(682) 207-9322**. According to the minor female victim, "**itsmeyall1**" provided the number in the event that there was a problem with the KIK Messenger application and they needed an alternate means to communicate.

27. When the minor female victim grew tired of the conversation and decided to stop sending photographs of herself, the user of "**itsmeyall1**" threatened to post the explicit photos of the minor female victim to her personal Facebook page. The minor female victim then stopped all further communication with the user of "**itsmeyall1**" and deleted the Kik Messenger application from her cellular phone. The minor female victim indicated she sent approximately twenty-five (25) images and videos of herself to the user of "**itsmeyall1.**"

28. In February of 2016, Constable Ken Samways, an officer with the RCMP sought and received a production order, pursuant to the Canadian Criminal Code, for the KIK Messenger service to provide subscriber information and stored content associated with the username "**itsmeyall1**". As a result of the production order served on the KIK Messenger service, the RCMP learned that the KIK Messenger user "**itsmeyall1**" had accessed the application from a cellular device, which was the assigned Internet Protocol (IP) address 172.56.6.240. In response to the production order, KIK Messenger also provided fifty-one (51) folders of digital content sent or received by KIK user "**itsmeyall1,**" many of which contained images previously known by law enforcement as

depicting child pornography, as defined in 18 U.S.C. § 2256. Specifically, located in two of the above mentioned 51 folders, were images of the previously referenced minor female victim engaged in sexually explicit conduct to include the lewd and lascivious exhibition of her genitals.

29. A commercial database search for the phone number (682) 207-9322 indicates the service provider is T-Mobile US, Inc., doing business as Metro PCS. A search for the IP address 172.56.6.240 also resolved to T-Mobile US, Inc.

30. In April of 2016, an administrative summons was served on T-Mobile requesting subscriber information associated with phone number (682) 207-9322. The returned information identified the subscriber as Pedro De Pacas of [redacted] Hallmark Drive, in Arlington, Texas. The summons return also indicated the cellular phone number has been assigned to Pedro De Pacas since November 4, 2013. The return also identified three separate cellular devices have been associated with the phone number since the phone number has been assigned to Pedro De Pacas. A review of local property records and commercial databases indicate both the name and address identified in the T-Mobile summons return are fictitious.

31. In October of 2016, an administrative summons was served on KIK Messenger requesting IP logs for the previous sixty days for the user "**itsmeyall1**." In response KIK Messenger provided logs indicating the application was most frequently accessed via T-Mobile/MetroPCS' wireless Internet service, which is consistent with the use of a MetroPCS "smart" cellular phone.

32. The KIK Messenger IP logs also indicated the KIK user "**itsmeyall1**" sporadically accessed the application from other Internet service providers, including an IP address associated with Charter Communications for approximately 20 minutes on October 14, 2016. Later the same day, the KIK user "**itsmeyall1**" accessed the application from an Internet protocol address resolving to Texas Health Resources for approximately two hours. Texas Health Resources is a network of 24 hospitals in the Dallas-Fort Worth area, which provide free wireless Internet access at many of their locations. Due to the KIK user's limited connection to these two Internet services, it is unlikely the two corresponding locations where the Internet was accessed are the KIK user's residence or place of employment.

33. On November 22, 2016, in the Northern District of Texas, I applied for and was granted a search warrant to be served on T-Mobile, which is the service provider for the cellular phone assigned phone number **(682) 207-9322** (hereinafter referred to as the Target Cellular Device). The search warrant compelled T-Mobile to provide E911 Phase 2 location data for the Target Cellular Device, which is the approximated near real-time latitude and longitude coordinates for the device. Since issuance and service of the search warrant, the Target Cellular Device has emitted E911 Phase 2 information indicating it has been and is presently located in the vicinity of 5003 Garden Drive, Hutchins, Dallas County, Texas.

34. On December 9, 2016, law enforcement officers with Homeland Security Investigations used an investigative device, specifically authorized pursuant to a separate federal search warrant issued in the Northern District of Texas, to confirm the Target Cellular Device's presence within the property located at 5003 Garden Drive, Hutchins, Texas.

35. On December 9, 2016, I conducted surveillance on the property located at 5003 Garden Drive, in Hutchins, Texas. During the surveillance I observed the property is made up of two distinct structures including the primary house and a detached garage, which appears to have been converted into an additional living space. While surveilling the property, I observed an adult male walk from the primary house to the detached garage. Additionally, after conferring with an officer at the Hutchins, Texas Police Department, I learned that there is only one water utility connection to the 5003 Garden Drive property. I am aware that like cellular phones, many computers and electronic storage devices today, such as laptop computers, tablets, external drives and thumb drives, are portable. I also know from my training and experience that these devices are often stored in vehicles to prevent other users in the home from discovering the existence of images or records related to the sexual exploitation of children. Therefore, this application seeks permission to search vehicles located at or near the premises that fall under the dominion and control of the person or persons associated with said premises. The search of these vehicles is to include all internal and external compartments and all containers that may be associated with materials related to the exploitation of children or their instrumentalities contained within the aforementioned vehicles.

CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

36. Based on my training and experience, and conversations with other law enforcement officials familiar with the traits and characteristics of child pornography collectors, I can attest that certain characteristics are generally found to exist in cases involving individuals who collect child pornography. These characteristics include the following:

a. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage of their collections of illicit materials.

b. The majority of individuals who collect child pornography often seek like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography as a means of gaining status, trust, acceptance and support. The different internet-based vehicles used by such individuals to communicate with each other include, but are not limited to: e-mail, e-mail groups, bulletin boards, forums, newsgroups, instant messaging, and other similar vehicles.

c. The majority of individuals who collect child pornography often store identifying information concerning child victims, as well as identifying information about other individuals who share the same interests.

d. Based on my training and experience, the suspect in this case appears to be a collector of child pornography. I base this opinion on the following:

i. The production order obtained by the Royal Canadian Mounted Police and served on KIK Interactive, resulted in the identification of fifty-one (51) folders of digital content sent or received by KIK user "**itsmeyall1**". I have personally reviewed a portion of the content contained within these folders and contained within these folders were both child pornography depicting the original complaining victim as well as numerous child pornography images, previously known by law enforcement officers to be widely traded on the Internet.

ii. The presence of the previously known child pornography images on the KIK account indicates the KIK user "**itsmeyall1**" not only produces new exploitative images through extortion, but also seeks out existing child pornography content.

CONCLUSION

37. Based on the aforementioned factual information, there is probable cause to believe that evidence, fruits, and instrumentalities may be located at the address described in Attachment A, in violation of 18 U.S.C. §§ 2252 and 2252A. Rule 41 of the Federal Rules of Criminal Procedure authorizes the government to seize and retain evidence and instrumentalities of a crime for a reasonable time, and to examine, analyze, and test them.

38. I, therefore, respectfully request that the attached warrant be issued authorizing the search of the location described in Attachment A and seizure of the items listed in Attachment B.

Kyle L. Kuykendall, Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on December 12, 2016, at 3:50 a.m./p.m. in Fort Worth, Texas.

JEFFREY L. CURETON
United States Magistrate Judge

ATTACHMENT A
DESCRIPTION OF ITEM TO BE SEARCHED

5003 Garden Drive, Hutchins, Texas 75172

The residence is described as a single-family, one-story residence, covered with blue siding and white trim. "5003" is displayed on the mail box on the sidewalk leading to the residence's front door. The house has a detached garage in the backyard, which appears to have been converted into an additional living space. This residence is located in Hutchins, Dallas County, which is within the Northern District of Texas.

The search also includes the search of vehicles located at or near the premises, which fall under the dominion and control of the person or persons associated with said premises. The search of these vehicles is to include all internal and external compartments and all containers that may be associated with the storage of child pornographic materials or their instrumentalities contained within the aforementioned vehicles.

ATTACHMENT B
DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

1. Computers, tablets, mobile devices/cellular phones, to include a cellular phone assigned the phone number (682) 207-9322, hard drives and computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Evidence of who used, owned, or controlled the Target Cellular Device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, accounts of Internet Service Providers.

3. Records evidencing occupancy of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence, rental or lease agreements, mortgage documents, rental or lease payments and credit card information, including, but not limited to, bills and payment records.

4. Any and all notes, documents, records, computer files or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail

messages, chat logs and electronic messages, and handwritten notes) pertaining to the production, possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the production, possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

5. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

6. Any and all cameras, film, videotapes or other photographic equipment.

7. During the execution of this search warrant, the law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of any person, who is located at the Subject Premises during the execution of the search and who is reasonably believed by law enforcement to be a user of a fingerprint sensor-enabled device that is located at the Subject Premises and falls within the scope of this warrant.